(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 824 732 B1

(12) FASCICULE DE BREVET EUROPEEN

(45) Date de publication et mention de la délivrance du brevet:
23.06.1999 Bulletin 1999/25

(21) Numéro de dépôt: **96914253.8**

(22) Date de dépôt: **26.04.1996**

(51) Int Cl.[6]: **G07C 15/00**, G06F 1/00

(86) Numéro de dépôt international:
PCT/FR96/00645

(87) Numéro de publication internationale:
WO 96/34368 (31.10.1996 Gazette 1996/48)

(54) PROCEDE D'ACTIVATION ET DE PROTECTION ANTI-FRAUDE D'UN DISPOSITIF ELECTRONIQUE DE JEU, ET DISPOSITIF CORRESPONDANT

AKTIVIERUNGS- UND SCHUTZVERFAHREN GEGEN DEN BETRUG BEI EINEM ELEKTRONISCHEN SPIELGERÄT UND DAZUGEHÖRIGES GERÄT

TAMPER PROTECTION AND ACTIVATION METHOD FOR AN ELECTRONIC GAMING DEVICE AND DEVICE THEREFOR

(84) Etats contractants désignés:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

(30) Priorité: **28.04.1995 FR 9505175**

(43) Date de publication de la demande:
25.02.1998 Bulletin 1998/09

(73) Titulaire: **INFO TELECOM**
67550 Vendenheim (FR)

(72) Inventeurs:
- **BERNHARD, François**
  F-67100 Strasbourg (FR)
- **BREMAUD, Patrice**
  F-67550 Vendenheim (FR)

(74) Mandataire: **Casalonga, Axel et al**
BUREAU D.A. CASALONGA - JOSSE
Morassistrasse 8
80469 München (DE)

(56) Documents cités:
EP-A- 0 360 613
EP-A- 0 547 975
EP-A- 0 596 760
WO-A-92/10806
US-A- 4 462 076
US-A- 4 882 473

EP 0 824 732 B1

Description

[0001] L'invention concerne l'activation et la protection anti-fraude d'un dispositif électronique de jeu et le dispositif correspondant.

[0002] On connaît actuellement différents jeux, notamment des jeux de hasard, permettant à un joueur de gagner des sommes d'argent moyennant le paiement d'une mise de départ. Ainsi, par exemple dans le jeu appelé "Loto" (marque déposée) le joueur coche une série de chiffres sur un ticket qu'il fait valider auprès d'un organisme spécialisé en acquittant un prix correspondant à la mise de départ. Un tirage au sort ultérieur est effectué sous contrôle dans un endroit choisi et, les joueurs en possession d'un ticket gagnant peuvent retirer leurs gains auprès d'un organisme payeur.

[0003] D'autres jeux consistent à se procurer un ticket et à gratter celui-ci en des endroits désignés de façon à découvrir des informations permettant de définir si le ticket en question est gagnant ou perdant.

[0004] Par rapport à ces jeux classiques nécessitant un support-papier, il a déjà été envisagé de proposer, dans le brevet français n° 92 13 239, un concept radicalement différent de dispositif de jeu de hasard.

[0005] Selon ce concept, il est prévu un boîtier portable destiné à permettre à un joueur d'effectuer une ou plusieurs épreuves de jeux de hasard, la réussite ou l'échec auxdites épreuves conditionnant un score ou un niveau de gain suivant des règles de jeu prédéterminées. Ce boîtier constitue alors également l'élément de transaction pour le paiement du gain et comporte tous les éléments nécessaires pour la vérification de celui-ci.

[0006] Cependant, de par sa conception et notamment pour des raisons de sécurité, chaque boîtier autonome ne peut être utilisé qu'une seule et unique fois. Ceci pose naturellement un problème économique et écologique en raison de cette utilisation unitaire combinée avec une diffusion estimée de l'ordre de plusieurs dizaines de millions d'unités par mois.

[0007] Outre le fait que ce type de boîtier ne peut être utilisé qu'une seule fois, il est par ailleurs associé à un type de jeu unique. Or, le marché actuel des jeux de hasard montre que la durée de vie d'un type de jeu est généralement courte et que ceux-ci doivent être renouvelés souvent ce qui conduit alors le fabricant du boîtier à concevoir en permanence de nouvelles formes extérieures pour le produit ainsi que de nouvelles interfaces logicielles.

[0008] L'invention vise à apporter une solution à ces problèmes.

[0009] Un but de l'invention est de proposer un dispositif électronique de jeu capable d'être utilisable plusieurs fois avec éventuellement différents types de jeu.

[0010] Un problème très important inhérent à de tels dispositifs de jeu réside dans la sécurité anti-fraude, en particulier lorsque certains types de jeu sont associés à des gains importants.

[0011] L'invention vise par conséquent à intégrer cette notion de sécurité dans un dispositif de jeu multi-applications et multi-utilisations.

[0012] L'invention, selon la revendication 1, propose donc tout d'abord un procédé d'activation et de protection anti-fraude d'un dispositif électronique de jeu comportant au moins un boîtier, ainsi qu'au moins un objet portatif capable de coopérer avec le boîtier. Selon ce procédé, on stocke dans le boitier au moins une clé de cryptage-résultat et on stocke dans l'objet portatif un ensemble de données numériques de jeu authentifiable et représentatif d'un jeu, on fait coopérer l'objet portatif avec le boîtier. On vérifie au sein du boîtier l'authentification de l'ensemble de données de jeu et on stocke cet ensemble de données de jeu dans une mémoire de travail du boîtier, de façon à autoriser le déroulement du jeu au niveau du boîtier. Puis, après le déroulement d'au moins une partie du jeu, on crypte au sein du boîtier une information de résultat dépendante dudit jeu, à l'aide au moins de ladite clé de cryptage-résultat. On stocke cette information de résultat cryptée dans une mémoire de résultat de l'objet portatif. Puis, on fait coopérer l'objet portatif avec une station de validation ayant accès à ladite clé de cryptage-résultat, ladite station effectuant un traitement de validation à partir au moins de ladite information de résultat cryptée et de ladite clé de cryptage-résultat.

[0013] Ainsi, selon l'invention, on déporte les données numériques de jeu, c'est-à-dire l'applicatif ou le logiciel de jeu, à l'extérieur du boîtier électronique et on l'incorpore dans une mémoire d'un objet portatif qui peut se présenter sous différentes formes, telles que carte de crédit, domino, jeton, etc.

[0014] Quant au boîtier électronique, celui-ci peut être vendu une seule fois et être utilisable plusieurs fois avec tout objet portatif contenant un logiciel de jeu.

[0015] Selon l'invention c'est donc l'objet portatif qui est destiné à contenir à la fois les données numériques de jeu définissant le jeu proprement dit, ainsi que l'information de résultat permettant au joueur de faire valider ce résultat de façon à toucher éventuellement son gain. En d'autres termes, l'objet portatif constitue ici l'élément de transaction tandis que le boîtier ne sert uniquement au joueur que pour jouer.

[0016] La notion de "cryptage" doit s'interpréter très largement comme étant une "protection à l'aide de moyens cryptographiques". Ceci étant, à des fins de simplification, seuls les termes cryptage, décryptage, crypter, décrypter seront employés dans la suite du texte.

[0017] L'information de résultat qui va être cryptée dans le boîtier avant d'être transférée dans l'objet portatif, dépend naturellement de la nature du jeu. Il peut s'agir par exemple d'une information binaire du type "gagné" ou "perdu", ou bien encore, par exemple, d'une information représentative d'un niveau de gain.

[0018] Pour des raisons de sécurité, l'ensemble de données numériques de jeu stocké dans l'objet portatif est authentifiable de façon à permettre la vérification de

son authentification au sein du boîtier. Au sens de la présente invention, le mot "authentifiable" doit être interprété de façon large incluant par exemple un stockage en "clair" des données numériques de jeu proprement dites conjointement à un certificat d'authentification obtenu, à partir de ces données numériques de jeu, par un algorithme approprié, ou bien encore un cryptage au moins partiel de cet ensemble, ou par exemple un cryptage du certificat d'authentification.

[0019] La vérification de l'authentification de l'ensemble de données de jeu peut s'effectuer avant, pendant ou après le stockage de celui-ci dans la mémoire de travail du boîtier.

[0020] Il convient également de remarquer ici que, selon l'invention, l'ensemble des données numériques de jeu est transféré dans la mémoire de travail du boîtier (en pratique ces données sont par exemple lues dans l'objet portatif puis recopiées dans la mémoire de travail du boîtier) de sorte que la coopération entre l'objet portatif et le boîtier pourrait éventuellement être supprimée pendant le déroulement du jeu au niveau du boîtier.

[0021] L'invention évite donc ainsi l'emploi de moyens logiciels complexes que nécessiterait l'exploitation directe du logiciel de jeu de l'objet portatif par l'unité de traitement du boîtier sans transfert dans la mémoire du boîtier. Aussi, selon un mode de mise en oeuvre du procédé selon l'invention, il est avantageusement prévu que l'ensemble de données de jeu d'un objet portatif soit lu par l'intermédiaire d'un protocole série entre l'objet portatif et le boîtier. Ce qui permet de minimiser les moyens matériels et logiciels de l'objet portatif. L'exploitation directe du logiciel de jeu s'effectue par l'unité de traitement du boîtier directement dans la mémoire de travail de celui-ci.

[0022] D'une façon très générale, le traitement de validation effectué par la station de validation doit permettre de déterminer et/ou de vérifier l'information de résultat à partir du contenu de l'objet portatif. En effet seul ce contenu mémorisé doit faire foi pour autoriser un paiement éventuel d'un gain.

[0023] Le traitement de validation effectué par la station de validation peut comporter un décryptage de l'information de résultat cryptée et stockée dans la mémoire de résultat de l'objet portatif, à l'aide de la clé de cryptage-résultat.

[0024] En variante, ce traitement de validation peut s'effectuer d'une manière différente. Plus précisément, on peut stocker dans l'objet portatif, conjointement avec l'information de résultat cryptée, l'information de résultat non cryptée c'est-à-dire "en clair". La station vérifie alors ladite information de résultat en recryptant, à l'aide de la clé de cryptage-résultat, l'information de résultat non cryptée qui est stockée dans l'objet portatif et en comparant cette information de résultat recryptée avec l'information de résultat cryptée et stockée dans la mémoire de résultat de l'objet portatif.

[0025] Afin d'augmenter encore la sécurité, il est avantageusement prévu que lorsque l'authentification de l'ensemble de données de jeu de l'objet portatif a été vérifié et que ledit ensemble a été stocké dans la mémoire du travail du boîtier, on interdise toute exploitation ultérieure par le boîtier, de l'ensemble de données de jeu de cet objet portatif.

[0026] Ceci permet notamment d'éviter qu'un joueur ne s'entraîne à jouer à un type de jeu, en particulier lorsque celui-ci est en fait un jeu de réflexe.

[0027] Au sens de la présente invention, l'interdiction de toute exploitation ultérieure doit s'entendre dans un sens très large signifiant par exemple que, soit le boîtier ne peut plus lire l'ensemble de données, soit il ne peut plus vérifier son authentification. En d'autres termes, le boîtier sera alors inapte au jeu avec cet objet portatif.

[0028] Le dispositif selon l'invention comprend généralement plusieurs boîtiers et plusieurs objets portatifs. Aussi, lorsque l'authentification de l'ensemble de données de jeu de l'un des objets portatifs a été vérifiée et que ledit ensemble a été stocké dans la mémoire de travail de l'un des boîtiers, on interdit alors avantageusement toute exploitation ultérieure par l'un quelconque des boîtiers, de l'ensemble de données de jeu de cet objet portatif.

[0029] Selon un mode de mise en oeuvre du procédé selon l'invention, on peut authentifier l'ensemble de données de jeu stocké dans l'objet portatif en y adjoignant un certificat d'authentification lié de façon biunivoque aux données numériques de jeu. La vérification de l'authentification de l'ensemble de données de jeu comporte alors un recalcul du certificat d'authentification au sein du boîtier et une comparaison entre le certificat d'authentification recalculé et le certificat d'authentification stocké dans l'objet portatif.

[0030] Ainsi, on peut interdire toute exploitation ultérieure d'un ensemble de données de jeu en altérant dans l'objet portatif correspondant, au moins partiellement ledit certificat d'authentification et/ou au moins partiellement les données de jeu proprement dites. On peut à cet effet envisager de modifier arbitrairement la valeur de certains des bits du certificat d'authentification et/ou de certaines des données numériques de jeu. De ce fait, si un joueur essaye de rejouer avec le même objet portatif, l'unité de traitement du boîtier recalculera un certificat d'authentification qui diffèrera du certificat d'authentification altéré, ce qui interdira toute activation du jeu.

[0031] Toujours dans le but d'augmenter la sécurité, notamment en ce qui concerne le paiement de gains éventuels, on autorise avantageusement le stockage de l'information de résultat cryptée dans l'objet portatif que si l'on a, au préalable, interdit toute exploitation ultérieure de l'ensemble de données de jeu de cet objet portatif.

[0032] Selon un mode de mise en oeuvre du procédé, on peut stocker dans le boîtier au moins une clé de cryptage-jeu.

[0033] L'authentification de l'ensemble de données de jeu stocké dans l'objet portatif peut comporter alors un cryptage au moins partiel de cet ensemble de don-

nées de jeu, ou d'une information reliée à cet ensemble de données de jeu (par exemple le certificat d'authentification), à l'aide de la clé de cryptage-jeu, et ce, avant lecture par l'unité de traitement du boîtier, de l'ensemble de données de jeu de l'objet portatif. La vérification de l'authentification de l'ensemble de données de jeu comporte alors un décryptage au sein du boîtier à l'aide de la clé de cryptage-jeu. En d'autres termes, le transfert crypté de l'applicatif, ou du certificat d'authentification associé, permet d'éviter le chargement d'un applicatif frauduleux conduisant inéluctablement à l'obtention d'un gain.

[0034] On peut éventuellement ne crypter et ne décrypter que le certificat d'authentification.

[0035] Lorsqu'une clé de cryptage-boîtier est stockée dans le boîtier, on peut stocker dans le boîtier la clé de cryptage-jeu qui a été au préalable cryptée à l'aide de la clé de cryptage-boîtier. Ceci permet encore d'augmenter la sécurité et de rendre encore plus difficile la connaissance par un tiers de la clé de cryptage-jeu.

[0036] La clé de cryptage-jeu peut être commune à tous les boîtiers et à tous les objets portatifs. La clé de cryptage-boîtier est quant à elle de préférence différente pour chaque boîtier. La clé de cryptage-boîtier d'un boîtier est stockée dans celui-ci avant le stockage de la clé de cryptage-jeu, par exemple lors de sa fabrication. Par ailleurs, l'ensemble de données de jeu d'un objet portatif peut être stocké dans celui-ci, déjà au moins partiellement crypté, ou associé à une information déjà au moins partiellement cryptée, à l'aide de la clé de cryptage-jeu. En d'autres termes, lors de la fabrication en usine des objets portatifs, on peut par exemple déterminer in situ le certificat d'authentification correspondant, crypter ce dernier, et stocker dans l'objet portatif, avant diffusion dans le public, les données de jeu proprement dites suivies de leur certificat d'authentification crypté.

[0037] D'une façon générale, la clé de cryptage-résultat peut être la clé de cryptage-boîtier, ou bien la clé de cryptage-jeu, ou bien être obtenue à partir d'une combinaison de ces deux clés.

[0038] Lorsque la clé de cryptage-résultat est la clé de cryptage-jeu, toute station de validation connaît cette clé de cryptage-jeu puisqu'elle est commune à tous les éléments du dispositif. Ceci étant, lorsque la clé de cryptage-résultat n'est pas connue à l'avance par la station de validation, il est prévu que l'on stocke dans l'objet portatif coopérant avec le boîtier, une information de clé associée de façon biunivoque à ladite clé de cryptage-résultat, la station de validation ayant alors accès à ladite clé de cryptage-résultat en lisant ladite information de clé stockée dans l'objet portatif.

[0039] Ainsi, si par exemple la clé de cryptage-résultat est la clé de cryptage-boîtier, il peut être avantageusement prévu d'associer à chaque boîtier un identifiant le définissant de façon unique, et permettant d'identifier par là même la clé de cryptage-boîtier qui a été stockée dans le boîtier. Une table d'identifiants peut être par exemple stockée de façon protégée dans un ordinateur central auquel sont reliées toutes les stations de validation. L'identifiant du boîtier est alors stocké avec l'information de résultat cryptée dans l'objet portatif. La station de validation ayant alors accès à l'identifiant ainsi qu'à la table de correspondance peut déterminer la clé de cryptage-résultat et décrypter l'information de résultat cryptée.

[0040] L'invention, selon la revendication 17, a également pour objet un dispositif électronique de jeu. Selon une caractéristique générale de l'invention, ce dispositif électronique de jeu comprend au moins un boîtier, au moins un objet portatif et au moins une station de validation. L'objet portatif comporte une mémoire de jeu contenant un ensemble de données de jeu authentifiable et représentatif d'un jeu, une mémoire de résultat apte à contenir une information de résultat cryptée, une première interface de communication apte à coopérer avec une interface de communication-boîtier, et une deuxième interface de communication apte à communiquer avec une interface de communication-station. Le boîtier comporte une mémoire de clé contenant au moins une clé de cryptage-résultat, une mémoire de travail accessible en écriture et en lecture, et une unité de traitement reliée à ces mémoires ainsi qu'à l'interface de communication-boîtier. L'unité de traitement est capable, lors d'une coopération entre l'interface de communication-boîtier et la première interface de communication de l'objet, de vérifier l'authentification de l'ensemble de données de jeu mémorisé dans l'objet et de stocker ledit ensemble dans la mémoire de travail de façon à permettre le déroulement du jeu au niveau du boîtier. L'unité de traitement du boîtier est également capable de crypter une information de résultat dépendante dudit jeu, à l'aide de la clé de cryptage-résultat, et de communiquer cette information de résultat cryptée à l'interface de communication-boîtier aux fins de son stockage dans la mémoire de résultat de l'objet. La station de validation comporte des moyens aptes à déterminer ladite clé de cryptage-résultat et des moyens de traitement-station aptes à lire l'information de résultat cryptée via l'interface de communication-station, lors d'une coopération entre l'objet portatif et la station, et à effectuer un traitement de validation à partir au moins de l'information de résultat cryptée et de la clé de cryptage-résultat.

[0041] Dans le cas où le dispositif électronique de jeu comprend plusieurs boîtiers, plusieurs objets portatifs et plusieurs stations de validation, l'un quelconque des objets portatif est capable de coopérer avec l'un quelconque des boîtiers et avec l'une quelconque des stations de validation.

[0042] Selon un mode de réalisation du dispositif selon l'invention, la première interface de communication de l'objet portatif est une interface série.

[0043] Par ailleurs, et pour des raisons d'économie, il est possible de prévoir que l'objet portatif ne comporte qu'une seule et même interface de communication capable de coopérer avec l'interface de communication-boîtier ou avec l'interface de communication-station.

[0044] Les moyens de traitement-station peuvent comporter des moyens de décryptage-station aptes à décrypter l'information de résultat cryptée aux fins de sa détermination.

[0045] En variante, l'unité de traitement du boîtier est apte à communiquer également l'information de résultat non cryptée à l'interface de communication-boîtier aux fins de son stockage dans la mémoire de résultat de l'objet. Les moyens de traitement-station sont alors en outre aptes à lire l'information de résultat non cryptée via l'interface de communication-station. Ils comportent alors des moyens de cryptage-station aptes à crypter ladite information de résultat non cryptée à l'aide de la clé de cryptage-résultat, ainsi que des moyens de comparaison pour comparer l'information de résultat cryptée recalculée, avec l'information de résultat cryptée stockée dans la mémoire de résultat de l'objet portatif. Cette comparaison permet ainsi de vérifier l'information de résultat.

[0046] Lorsque l'ensemble de données de jeu authentifiable est associé à un certificat d'authentification, les moyens de vérification de l'authentification de cet ensemble de données de jeu comportent alors de préférence des moyens de calcul de certificat aptes à recalculer ledit certificat d'authentification au sein du boîtier, à partir de l'ensemble de données de jeu, et des moyens de comparaison apte à comparer le certificat recalculé et le certificat stocké dans la mémoire de jeu de l'objet portatif.

[0047] Selon un mode de réalisation du dispositif, il est possible de prévoir des moyens de cryptage apte à crypter au moins partiellement l'ensemble de données de jeu authentifiable, ou une information reliée à cet ensemble de données de jeu (par exemple le certificat d'authentification), à partir d'au moins une clé de cryptage-jeu. La mémoire de clé du boîtier est alors apte à contenir cette clé de cryptage-jeu tandis que les moyens de vérification de l'authentification de l'ensemble de données de jeu comportent des moyens de décryptage reliés à la mémoire de clé. Ces moyens de cryptage peuvent ne crypter que le certificat d'authentification.

[0048] Ces moyens de cryptage peuvent être incorporés au sein d'une unité de fabrication de façon à délivrer directement un ensemble de données de jeu au moins partiellement crypté ou un certification d'authentification déjà au moins partiellement crypté, qui sera destiné à être stocké tel quel dans l'objet portatif. Cependant, on peut prévoir en variante que les moyens de cryptage soient incorporés à l'objet portatif, notamment lorsque celui-ci comporte un micro-contrôleur contenant de façon logicielle ces moyens de cryptage.

[0049] De même, le fait de prévoir un objet portatif "intelligent", c'est-à-dire pourvu d'une unité centrale par exemple, permet également d'incorporer dans l'objet portatif des moyens permettant d'interdire toute exploitation ultérieure d'un ensemble de données de jeu d'un objet portatif après une première exploitation. Ce moyens, qui peuvent être réalisés par exemple de façon logicielle, sont ainsi par exemple aptes à modifier la valeur de certains des bits de l'ensemble de données de jeu ou de son certificat d'authentification.

[0050] D'autres avantages et caractéristiques de l'invention apparaîtront à l'examen de modes de mise en oeuvre et de réalisation de l'invention, nullement limitatifs, et des dessins annexés sur lesquels :

- la figure 1 représente très schématiquement l'architecture matérielle d'un objet portatif d'un dispositif selon l'invention,
- la figure 2 représente très schématiquement l'architecture matérielle d'un boîtier du dispositif selon l'invention,
- la figure 3 représente très schématiquement l'architecture matérielle d'une station de validation du dispositif selon l'invention,
- les figures 4a et 4b illustrent schématiquement un mode de mise en oeuvre du procédé selon l'invention, et
- les figures 5 et 6 illustrent deux variantes de mise en oeuvre du procédé selon l'invention.

[0051] Le dispositif selon l'invention comporte plusieurs boîtier électroniques autonomes BT, plusieurs objets portatifs OB et plusieurs stations de validation ST.

[0052] Tel qu'illustré sur la figure 1, chaque objet portatif OB, par exemple une carte du type carte à puce, un jeton, ou un module, comporte, par exemple au sein d'un ASIC (Application Specific Integrated Circuit) un micro-contrôleur CPU relié par l'intermédiaire d'un bus à une interface d'entrée sortie ESC du type série, à une mémoire de jeu MJ, ainsi qu'à une mémoire de résultat MR, telle qu'un registre.

[0053] Comme on le verra plus en détail ci-après, la mémoire de jeu MJ, par exemple une mémoire morte, est destinée à recevoir un ensemble de données numériques de jeu, ou logiciel de jeu, représentatif d'un type particulier de jeu.

[0054] Le registre MR est destiné quant à lui à recevoir une information de résultat cryptée provenant du boîtier BT après le déroulement d'au moins une partie du jeu.

[0055] L'interface ESC comporte des moyens de coopération avec une interface homologue ESB du boîtier BT (figure 2) et une interface homologue ESS de la station ST (figure 3). Ces moyens de coopération peuvent consister en un connecteur mécanique ou bien en des moyens de couplage capacitif/inductif, ou optique.

[0056] Comme illustrée plus particulièrement sur la figure 2, la structure électronique matérielle du boîtier portable BT s'articule autour d'une unité de traitement UT, telle qu'un microprocesseur ou un micro-contrôleur. Cette unité de traitement UT est reliée par l'intermédiaire d'un bus à une mémoire de travail MT, accessible en écriture et en lecture, par exemple une mémoire à accès aléatoire (RAM), à une mémoire de programme MM ainsi qu'à une mémoire type de clé MC qui est une mémoire

protégée pouvant être une partie de la mémoire MM.

[0057] L'unité de traitement est également reliée à un écran d'affichage à cristaux liquides AF ainsi qu'à un clavier Cl comportant par exemple des touches de commande de mouvements dans deux directions orthogonales. Enfin, l'unité de traitement est reliée à une interface de communication-boîtier ESB apte à coopérer avec l'interface de communication ESC, et pouvant par exemple comporter un connecteur mécanique disposé dans un logement dans lequel peut être inséré le connecteur de l'objet portatif. L'interface ESB comporte également des moyens de conversion série/parallèle reliés au bus interne du boîtier.

[0058] L'ensemble des moyens de ce boîtier est alimenté par des moyens d'alimentation autonomes AL tels que des piles. Tout ou partie des composants de ce boîtier peuvent être réalisés sous la forme d'un Asic.

[0059] La mémoire de travail MT est dimensionnée de façon à pouvoir recevoir l'applicatif de jeu stocké dans la mémoire MJ de l'objet tandis que la mémoire MM contient le programme de gestion interne du boîtier (gestion des entrées/sorties, gestion du clavier, de l'écran, programme de chargement de l'applicatif dans la mémoire de travail...).

[0060] Selon l'exemple de réalisation décrit en référence à la figure 3, chaque station de validation ST comporte un bloc de traitement articulé autour d'un processeur PR relié à une interface d'entrée/sortie ESS capable de coopérer avec l'interface d'entrée sortie ESC de l'objet portatif. Par ailleurs, la station est reliée par l'intermédiaire d'une liaison appropriée, à un fichier central TB contenant des informations nécessaires, comme on le verra plus en détail ci-après, à la vérification de l'information de résultat contenue dans l'objet portatif.

[0061] Le processeur PR de la station incorpore de façon logicielle les différents moyens fonctionnels nécessaires au fonctionnement de celle-ci (cryptage, décryptage, comparaison, lecture...).

[0062] On va maintenant décrire plus en détail, en se référant particulièrement aux figures 4a à 4b, un premier mode de mise en oeuvre du procédé selon l'invention.

[0063] Sur un site de fabrication, l'ensemble de données de jeu numériques JE, formant le logiciel applicatif de jeu, est traité par des moyens de traitement comportant un algorithme de calcul de certificat d'authentification du type SHA (Secure Hash Algorithm) bien connu de l'homme du métier. Ce dernier pourra cependant, pour plus de détails, se référer à la publication 180-1 du 31 mai 1994 diffusée par le FIPS (Federal Information Processing Standards).

[0064] Ces moyens de calcul déterminent un certificat d'authentification CTF à partir de fonctions logiques opérant sur les bits des données numériques de jeu (étape 1). Ainsi, pour un bloc de 1 kilo octet d'applicatif, le certificat d'authentification comporte par exemple 120 bits.

[0065] A partir d'une clé de cryptage-jeu Km, commune à tous les objets portatifs, à tous les boîtiers et à toutes les stations de validation, des moyens de cryptage, par exemple utilisant l'algorithme de cryptage DES (Data Encryption Standard) effectuent un cryptage du certificat d'authentification CTF (étape 2) de façon à délivrer un certificat d'authentification crypté CTFc. Les données numériques de jeu et le certificat d'authentification crypté sont alors stockés dans la mémoire de jeu MJ de l'objet portatif (étape 3).

[0066] L'objet portatif est alors prêt à être diffusé dans le public.

[0067] Quant au boîtier, on stocke dans la mémoire de clé MC de celui-ci, par exemple lors de sa fabrication sur site, une clé de cryptage-boîtier Kf (étape 4). Le boîtier est alors également prêt à être diffusé dans le public.

[0068] Un joueur peut se procurer un tel boîtier auprès d'une station de validation du type de la station ST. Lors de cette opération, on fait coopérer le boîtier et la station par l'intermédiaire d'interfaces de communication respectives de façon à lire (étape 5) la clé de cryptage-bo`94 tier Kf stockée dans la mémoire de clé du boîtier. Ces interfaces peuvent être, notamment quand elles sont du type à couplage capacité/inductif, les mêmes que les interfaces ESB et ESS. Elles peuvent être également distinctes de ces dernières, par exemple du type mécanique à connecteurs. Le processeur PR de la station de validation connaissant la clé de cryptage-jeu Km, (par exemple stockée dans le fichier central TB) effectue alors par l'intermédiaire de moyens de cryptage du type DES un cryptage (étape 6) de la clé Km à l'aide de la clé de cryptage/boîtier Kf. Cette clé de cryptage-jeu cryptée sous Kf, et référencée Kmc, est alors stockée (étape 7) dans la mémoire de clé du boîtier.

[0069] Lorsque le joueur souhaite jouer à un jeu particulier, il se procure auprès d'un détaillant spécialisé un objet portatif contenant le logiciel de jeu correspondant. Le joueur insère alors l'objet portatif dans le logement correspondant du boîtier de façon à faire coopérer les interfaces respectives ESC et ESB de l'objet et du boîtier.

[0070] Les moyens de décryptage, par exemple du type DES, incorporés de façon logicielle dans l'unité de traitement UT du boîtier décryptent la clé de cryptage-jeu crypté Kmc. L'unité de traitement lit les données numériques de jeu ainsi que le certificat d'authentification crypté CTFc stockés dans l'objet portatif, par l'intermédiaire d'un protocole série via l'interface ESB. L'unité de traitement UT recalcule alors un certificat d'authentification à partir des données numériques de jeu JE, décrypte le certificat d'authentification crypté CTFc à l'aide de la clé de cryptage-jeu Km, compare le certificat d'authentification recalculé et le certificat d'authentification stocké de façon à vérifier l'authenticité du logiciel de jeu (étape 8).

[0071] L'ensemble de données numériques de jeu JE est stocké dans la mémoire de travail MT du boîtier de façon à pouvoir être exploité ultérieurement et directement par l'unité de traitement UT aux fins d'exécution du jeu.

[0072] Il convient de noter ici que, notamment lorsqu'on utilise un certificat de type SHA, la vérification de l'authentification du logiciel de jeu JE peut se faire soit "au fil de l'eau", soit lorsque l'ensemble du logiciel a été transféré dans la mémoire de travail MT, cette dernière solution nécessitant une plus grande capacité de mémoire vive.

[0073] A ce stade, le boîtier est apte au jeu et le joueur peut jouer à l'aide de son boîtier (étape 9).

[0074] A la fin du jeu, ou en cours de celui-ci selon le type de jeu employé ou l'issue de celui-ci, une information de résultat IFR est délivrée par le logiciel de jeu, et celle-ci est cryptée (étape 10) par l'unité de traitement UT en utilisant une clé de cryptage-résultat qui est, dans le cas présent, identique à la clé de cryptage-jeu Km. On obtient alors une information de résultat cryptée IFRc qui est transférée via les interfaces respectives du boîtier et de l'objet portatif de façon à être stockée (étape 11) dans la mémoire de résultat MR de l'objet.

[0075] Le joueur peut alors aller faire valider son résultat de façon à toucher éventuellement son gain.

[0076] Pour ce faire, le joueur retire l'objet portatif du boîtier, et le communique à une station de validation, qui peut être la même que celle auprès de laquelle il s'est procuré son boîtier, ou bien une autre. On établit alors une coopération entre l'objet portatif et la station. Le processeur PR de la station lit alors dans la mémoire de résultat de l'objet portatif (étape 12) l'information de résultat cryptée IFRc et les moyens de décryptage de cette station, par exemple du type DES, connaissant la clé de cryptage-jeu Km, décryptent l'information IFRc de façon à obtenir l'information de résultat IFR et permettre le paiement du gain.

[0077] Si le joueur décide ultérieurement de jouer à nouveau, il lui suffit de se procurer un autre objet portatif contenant un jeu du même type ou d'un type différent et de le faire coopérer avec son boîtier pour jouer.

[0078] Dans la variante de mise en oeuvre illustrée sur la figure 5, et destinée à augmenter la sécurité du dispositif, il est prévu une altération 20 du certificat d'authentification crypté CTFc de l'objet portatif après que la vérification de l'authentification du logiciel de jeu a été effectuée par l'unité de traitement du boîtier. Cette altération consiste par exemple en une modification de la valeur de certains au moins des bits du certificat d'authentification.

[0079] Par ailleurs, avant de stocker l'information de résultat cryptée IFRc dans la mémoire de résultat de l'objet, on vérifie si cette altération a eu lieu (étape 21). Dans l'affirmative, on autorise le stockage dans la mémoire de résultat MR et dans la négative, on interdit ce stockage.

[0080] D'une façon générale, l'objet portatif est alimenté par l'intermédiaire du boîtier ou de la station. Toutes les fonctions qui viennent d'être décrites en relation avec les données stockées ou à stocker dans l'objet portatif, notamment l'altération du certificat d'authentification, peuvent être effectuées directement de façon logicielle par l'unité de traitement du boîtier. Dans ce cas, le microprocesseur CPU de l'objet portatif peut être omis. Ceci étant, l'existence d'un tel microprocesseur permet d'effectuer ces opérations d'altération (ou d'invalidation) et de vérification d'altération puis d'interdiction éventuelle d'écriture de l'information de résultat cryptée, directement au niveau de l'objet portatif. De même, l'existence d'un microprocesseur CPU sur l'objet portatif permet éventuellement un cryptage du logiciel de jeu au niveau de l'objet portatif avant transfert dans la mémoire de travail du boîtier.

[0081] Il se peut également que la clé de cryptage-résultat utilisée pour crypter l'information de résultat ne soit pas la clé de cryptage-jeu Km et ne soit pas connue à l'avance par la station de validation. Il peut en être ainsi lorsque la clé de cryptage-résultat est tout simplement la clé de cryptage-boîtier Kf. Dans ce cas, le mode de mise en oeuvre illustré sur la figure 6 prévoit non seulement le stockage de l'information de résultat cryptée IFRc dans la mémoire de résultat de l'objet (étape 11) mais aussi le stockage, dans cette mémoire de résultat ou dans une autre mémoire (étape 30, d'une information de clé ICR permettant ultérieurement de déterminer la clé de cryptage-résultat qui a été utilisée pour crypter l'information de résultat.

[0082] Cette information ICR peut être par exemple la clé de cryptage-résultat proprement dite ou bien un identifiant du boîtier qui est associé de façon biunivoque au boîtier et par conséquent à la clé de cryptage-boîtier Kf qui a été stockée.

[0083] Le processeur de la station de validation lit alors (étape 31) l'information de clé ICR et détermine à partir d'une table de correspondance entre les identifiants et les clés de cryptage-boîtier, stockée, de préférence de façon protégée, dans le fichier TB, la clé de cryptage-résultat Kr (en l'espèce la clé Kf) qui a été utilisée (étape 32).

[0084] Il peut être ensuite procédé au décryptage de l'information de résultat (étape 13).

[0085] Cette variante de l'invention permet en outre d'identifier précisément les boîtiers ayant conduit à des jeux gagnants et d'effectuer éventuellement des statistiques. Ceci offre une possibilité supplémentaire de détection d'une fraude éventuelle si l'on s'aperçoit qu'un même boîtier conduit très souvent à des jeux gagnants.

Revendications

1. Procédé d'activation et de protection anti-fraude d'un dispositif électronique de jeu comportant au moins un boîtier (BT), ainsi qu'au moins un objet portatif (OB) capable de coopérer avec le boîtier, procédé dans lequel on stocke dans le boîtier au moins une clé de cryptage-résultat et on stocke dans l'objet portatif un ensemble de données numériques de jeu authentifiable (JE) et représentatif d'un jeu, on fait coopérer l'objet portatif avec le boî-

tier, on vérifie (8) au sein du boîtier l'authentification de l'ensemble de données de jeu et on stocke cet ensemble de données de jeu dans une mémoire de travail (MT) du boîtier, de façon à autoriser le déroulement (9) du jeu au niveau du boîtier, puis, après le déroulement d'au moins une partie du jeu, on crypte (10) au sein du boîtier une information de résultat (IFR) dépendante dudit jeu à l'aide au moins de ladite clé de cryptage-résultat, et on stocke (11) cette information de résultat cryptée (IFRc) dans une mémoire de résultat (MR) de l'objet portatif, puis, on fait coopérer l'objet portatif avec une station de validation (ST) ayant accès à ladite clé de cryptage-résultat, ladite station effectuant un traitement de validation (13) à partir au moins de ladite information de résultat cryptée et de ladite clé de cryptage-résultat.

2. Procédé selon la revendication 1, caractérisé par le fait que le traitement de validation comporte un décryptage de l'information de résultat cryptée.

3. Procédé selon la revendication 1, caractérisé par le fait qu'on stocke dans l'objet portatif, conjointement avec l'information de résultat cryptée, l'information de résultat non cryptée, et par le fait que le traitement de validation comporte un recryptage de l'information de résultat non cryptée stockée dans l'objet portatif et une comparaison de cette information de résultat recryptée avec l'information de résultat cryptée et stockée dans la mémoire de résultat de l'objet portatif.

4. Procédé selon l'une des revendications 1 à 3, caractérisé par le fait que lorsque l'authentification de l'ensemble de données de jeu de l'objet portatif a été vérifiée et que ledit ensemble a été stocké dans la mémoire de travail du boîtier, on interdit (20) toute exploitation ultérieure, par le boîtier, de l'ensemble de données de jeu de cet objet portatif.

5. Procédé selon la revendication 4, caractérisé par le fait que, le dispositif comprenant plusieurs boîtiers et plusieurs objets portatifs, lorsque l'authentification de l'ensemble de données de jeu de l'un des objets portatifs a été vérifiée et que ledit ensemble a été stocké dans la mémoire de travail de l'un des boîtiers, on interdit toute exploitation ultérieure, par l'un quelconque des boîtiers, de l'ensemble de données de jeu de cet objet portatif.

6. Procédé selon l'une des revendications précédentes, caractérisé par le fait qu'on authentifie l'ensemble de données de jeu stocké dans l'objet portatif en lui adjoignant un certificat d'authentification (CTF) lié de façon biunivoque audit ensemble de données de jeu (JE) et par le fait que la vérification de l'authentification de l'ensemble de données de jeu comporte un recalcul du certificat d'authentification au sein du boîtier et une comparaison entre le certificat d'authentification recalculé et le certificat d'authentification stocké dans l'objet portatif.

7. Procédé selon la revendication 4 ou 5 prise en combinaison avec la revendication 6, caractérisé par le fait qu'on interdit toute exploitation ultérieure d'un ensemble de données de jeu en altérant, dans l'objet portatif correspondant, au moins partiellement ledit certificat d'authentification et/ou au moins partiellement l'ensemble de données de jeu.

8. Procédé selon l'une des revendications précédentes prise en combinaison avec la revendication 4, caractérisé par le fait qu'on autorise (21) le stockage de l'information de résultat cryptée dans l'objet portatif que si l'on a, au préalable, interdit toute exploitation ultérieure de l'ensemble de données de jeu de cet objet portatif.

9. Procédé selon l'une des revendications précédentes, caractérisé par le fait que l'on stocke dans le boîtier une clé de cryptage-boîtier (Kf).

10. Procédé selon l'une des revendications précédentes, caractérisé par le fait qu'on stocke dans le boîtier au moins une clé de cryptage-jeu (Km), par le fait que l'authentification de l'ensemble de données de jeu stocké dans l'objet portatif comporte un cryptage au moins partiel de cet ensemble de données de jeu, ou d'une information (CTF) reliée à cet ensemble de données de jeu, à l'aide de la clé de cryptage-jeu (Km), avant lecture par le boîtier, et par le fait que la vérification de l'authentification de cet ensemble de données de jeu comporte un décryptage au sein du boîtier à l'aide de la clé de cryptage-jeu.

11. Procédé selon les revendications 6 et 10, caractérisé par le fait que l'on crypte et on décrypte uniquement le certificat d'authentification (CTF).

12. Procédé selon la revendication 9 prise en combinaison avec la revendication 10 ou 11, caractérisé par le fait que l'on stocke dans le boîtier la clé de cryptage-jeu (Km) ayant été cryptée à l'aide de la clé de cryptage-boîtier (Kf).

13. Procédé selon la revendication 9 prise en combinaison avec l'une des revendications 10 à 12, caractérisé par le fait que, le dispositif comportant plusieurs boîtiers et plusieurs objets portatifs, une clé de cryptage-boîtier (Kf) différente est associée à chaque boîtier tandis que la clé de cryptage-jeu (Km) est commune pour tous les boîtiers et à tous les objets portatifs, par le fait que la clé de cryptage-boîtier d'un boîtier est stockée dans celui-ci avant le stockage de la clé de cryptage-jeu, et par le fait

que l'ensemble de données de jeu d'un objet portatif est stocké dans celui-ci, déjà au moins partiellement crypté, ou associé à une information (CTFc) déjà au moins partiellement cryptée, à l'aide la clé de cryptage-jeu.

14. Procédé selon la revendication 9 ou l'une des revendications 10 à 13, caractérisé par le fait que la clé de cryptage-résultat (Kr) est la clé de cryptage-boîtier (Kf), ou la clé de cryptage-jeu (Km), ou est obtenue à partir d'une combinaison de la clé de cryptage-boîtier et de la clé de cryptage-jeu.

15. Procédé selon l'une des revendications précédentes, caractérisé par le fait que l'on stocke dans l'objet portatif coopérant avec le boîtier, une information de clé (ICR) associée de façon biunivoque à ladite clé de cryptage-résultat, et par le fait que la station de validation a accès à ladite clé de cryptage-résultat en lisant ladite information de clé stockée dans l'objet portatif.

16. Procédé selon l'une des revendications précédentes, caractérisé par le fait que l'ensemble de données de jeu (JE) d'un objet portatif est lu par l'intermédiaire d'un protocole série entre l'objet portatif et le boîtier.

17. Dispositif électronique de jeu, caractérisé par le fait qu'il comprend au moins un boîtier (BT), au moins un objet portatif (OB), et au moins une station de validation (ST), par le fait que l'objet portatif comporte une mémoire de jeu (MJ) contenant un ensemble de données de jeu (JE) authentifiable et représentatif d'un jeu, une mémoire de résultat (MR) apte à contenir une information de résultat cryptée (IFRc), une première interface de communication (ESC) apte à coopérer avec une interface de communication-boîtier (ESB), et une deuxième interface de communication (ESC) apte à communiquer avec une interface de communication-station (ESS), par le fait que le boîtier comporte une mémoire de clé (MC) contenant une clé de cryptage-résultat, une mémoire de travail (MT) accessible en écriture et en lecture, et une unité de traitement (UT) reliée à ces mémoires ainsi qu'à l'interface de communication-boîtier, l'unité de traitement étant capable, lors d'une coopération entre l'interface de communication-boîtier et la première interface de communication de l'objet, de vérifier l'authentification de l'ensemble de données de jeu mémorisé dans l'objet et de stocker ledit ensemble dans la mémoire de travail de façon à permettre le déroulement du jeu au niveau du boîtier, puis de crypter une information de résultat (IFR) dépendante dudit jeu, à l'aide de la clé de cryptage-résultat, et de communiquer cette information de résultat cryptée (IFRc) à l'interface de communication-boîtier aux fins de son stockage dans la mémoire de résultat de l'objet, et par le fait que la station de validation (ST) comporte des moyens (PR) aptes à déterminer ladite clé de cryptage-résultat et des moyens de traitement-station (PR) aptes à lire l'information de résultat cryptée via l'interface de communication-station, lors d'une coopération entre l'objet portatif et la station, et à effectuer un traitement de validation à partir au moins de cette information de résultat cryptée et de la clé de cryptage-résultat.

18. Dispositif selon la revendication 17, caractérisé par le fait que les moyens de traitement-station comportent des moyens de décryptage-station aptes à décrypter l'information de résultat cryptée.

19. Dispositif selon la revendication 17, caractérisé par le fait que l'unité de traitement du boîtier est apte à communiquer également l'information de résultat non-cryptée à l'interface de communication-boîtier aux fins de son stockage dans la mémoire de résultat de l'objet, et par le fait que les moyens de traitement-station sont en outre aptes à lire l'information de résultat non cryptée via l'interface de communication-station, et comportent des moyens de cryptage-station aptes à crypter ladite information de résultat non cryptée à l'aide de la clé de cryptage-résultat, ainsi que des moyens de comparaison pour comparer l'information de résultat cryptée recalculée avec l'information de résultat cryptée stockée dans la mémoire de résultat de l'objet portatif.

20. Dispositif selon l'une des revendications 17 à 19, caractérisé par le fait que la première interface de communication (SEC) de l'objet portatif est une interface série.

21. Dispositif selon l'une des revendications 17 à 20, caractérisé par le fait que l'ensemble de données de jeu authentifiable est associé à un certificat d'authentification et par le fait que les moyens de vérification de l'authentification de cet ensemble de données de jeu comportent des moyens de calcul de certificat aptes à recalculer ledit certificat d'authentification à partir de l'ensemble de données de jeu, et des moyens de comparaison aptes à comparer le certificat recalculé et le certificat stocké dans la mémoire de jeu de l'objet portatif.

22. Dispositif selon l'une des revendications 17 à 21, caractérisé par le fait qu'il comprend des moyens de cryptage aptes à crypter au moins partiellement l'ensemble de données de jeu authentifiables (JE), ou une information (CTF) reliée à cet ensemble de données de jeu, à partir d'au moins une clé de cryptage-jeu, et par le fait que la mémoire de clé du boîtier est apte à contenir ladite clé de cryptage-jeu tandis que les moyens de vérification de l'authenti-

fication de l'ensemble de données de jeu comportent des moyens de décryptage reliés à la mémoire de clé.

23. Dispositif selon les revendications 21 et 22, caractérisé par le fait que les moyens de cryptage cryptent uniquement le certificat d'authentification (CTF).

24. Dispositif selon la revendication 22 ou 23, caractérisé par le fait que les moyens de cryptage (CPU) sont incorporés à l'objet portatif.

25. Dispositif selon l'une des revendications 22 à 24, caractérisé par le fait que la clé de cryptage-jeu est stockée cryptée et par le fait que l'unité de traitement (UT) du boîtier comporte des moyens de décryptage de cette clé de cryptage-jeu.

26. Dispositif selon l'une des revendications 17 à 25, caractérisé par le fait qu'il comprend des moyens (CPU) d'invalidation de l'ensemble de données de jeu authentifiable d'un objet portatif.

27. Dispositif selon l'une des revendications 17 à 26, caractérisé par le fait qu'il comprend des moyens (CPU) d'interdiction de l'écriture de l'information de résultat cryptée dans la mémoire de résultat de l'objet portatif.

28. Dispositif selon la revendication 26 ou 27, caractérisé par le fait que les moyens d'invalidation (CPU) et/ou les moyens d'interdiction (CPU) sont incorporés dans l'objet portatif.

29. Dispositif selon l'une des revendications 17 à 28, caractérisé par le fait qu'il comprend plusieurs boîtiers, plusieurs objets portatifs et plusieurs stations de validation, l'un quelconque des objets portatifs étant capable de coopérer avec l'un quelconque des boîtiers et avec l'une quelconque des stations de validation.

Patentansprüche

1. Verfahren zum Aktivieren und zum Schützen vor Betrug eines elektronischen Spielgerätes mit wenigstens einem Gehäuse (BT) und wenigstens einem tragbaren Gegenstand (OB), der mit dem Gehäuse zusammenarbeiten kann, bei welchem Verfahren man im Gehäuse wenigstens einen Schlüssel zur Ergebnisverschlüsselung speichert und im tragbaren Gegenstand einen Satz numerischer Daten (JE) eines Spiels, dessen Echtheit bestätigbar ist, und der ein Spiel wiedergibt, speichert, man den tragbaren Gegenstand mit dem Gehäuse zusammenarbeiten läßt, man im Inneren des Gehäuses die Echtheit des Datensatzes des Spieles prüft (8) und man diesen Datensatz des Spieles in einem Arbeitsspeicher (MT) des Gehäuses speichert, um den Ablauf (9) des Spieles auf der Höhe des Gehäuses zu autorisieren, woraufhin man nach dem Ablauf wenigstens eines Teils des Spiels im Inneren des Gehäuses eine Ergebnisinformation (IFR), die von dem Spiel abhängig ist, mittels wenigstens des besagten Schlüssels zur Ergebnisverschlüsselung verschlüsselt (10) und man diese verschlüsselte Ergebnisinformation (IFRc) in einem Ergebnisspeicher (MR) des tragbaren Gegenstandes speichert, woraufhin man den tragbaren Gegenstand mit einer Gültigmachungsstation (ST) zusammenarbeiten läßt, die Zugriff auf den besagten Schlüssel der Ergebnisverschlüsselung hat, welche Station eine Gültigkeitsbehandlung (13) ausgehend von wenigstens der besagten verschlüsselten Ergebnisinformation und dem besagten Schlüssel der Ergebnisverschlüsselung ausführt.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Gültigkeitsbehandlung eine Entschlüsselung der verschlüsselten Ergebnisinformation umfaßt.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß man im tragbaren Gegenstand gemeinsam mit der verschlüsselten Ergebnisinformation die nicht verschlüsselte Ergebnisinformation speichert und daß die Gültigkeitsbehandlung eine Nachverschlüsselung der nicht verschlüsselten im tragbaren Gegenstand gespeicherten Ergebnisinformation und einen Vergleich dieser nachverschlüsselten Ergebnisinformation mit der verschlüsselten und im Ergebnisspeicher des tragbaren Gegenstandes gespeicherten Ergebnisinformation umfaßt.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß man nach der Bestätigung der Echtheit des Datensatzes des Spieles vom tragbaren Gegenstand und nach dem Speichern dieses Datensatzes im Arbeitsspeicher des Gehäuses jede spätere Nutzung des Datensatzes des Spieles des tragbaren Gegenstandes durch das Gehäuse verbietet (20).

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß das Gerät mehrere Gehäuse und mehrere tragbare Gegenstände umfaßt und daß man nach der Bestätigung der Echtheit des Datensatzes des Spieles von einem tragbaren Gegenstand und nach der Speicherung dieses Datensatzes im Arbeitsspeicher eines Gehäuses jede weitere Nutzung des Datensatzes des Spieles des tragbaren Gegenstandes durch eines der Gehäuse verbietet.

6. Verfahren nach einem der vorhergehenden Ansprü-

che, dadurch gekennzeichnet, daß man den Datensatz des Spieles, der im tragbaren Gegenstand gespeichert ist, dadurch für echt erklärt, daß man diesem ein Echtheitszertifikat (CTF) anfügt, das eineindeutig mit dem Datensatz des Spieles (JE) verbunden ist, und daß die Prüfung der Echtheit des Datensatzes des Spieles eine Neuberechnung des Echtheitszertifikates im Gehäuse und einen Vergleich zwischen dem neuberechneten Echtheitszertifikat und dem im tragbaren Gegenstand gespeicherten Echtheitszertifikat umfaßt.

7. Verfahren nach Anspruch 4 oder 5 in Kombination mit Anspruch 6, dadurch gekennzeichnet, daß man jede spätere Nutzung eines Datensatzes des Spieles dadurch verbietet, daß man im entsprechenden tragbaren Gegenstand wenigstens teilweise das Echtheitszertifikat und/oder wenigstens teilweise den Datensatz des Spieles ändert.

8. Verfahren nach einem der vorhergehenden Ansprüche in Kombination mit Anspruch 4, dadurch gekennzeichnet, daß man die Speicherung der verschlüsselten Ergebnisinformation im tragbaren Gegenstand zuläßt (21), nachdem man vorher jede weitere Nutzung des Datensatzes des Spieles vom tragbaren Gegenstand verboten hat.

9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß man im Gehäuse einen Schlüssel zur Gehäuseverschlüsselung (Kf) speichert.

10. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß man im Gehäuse wenigstens einen Schlüssel der Spielverschlüsselung (Km) speichert, daß die Echtheitsprüfung des Datensatzes des Spieles, der im tragbaren Gegenstand gespeichert ist, eine Verschlüsselung wenigstens teilweise dieses Datensatzes des Spieles oder einer Information (CTF) umfaßt, die mit diesem Datensatz des Spieles verbunden ist, und zwar mittels des Schlüssels zur Spielverschlüsselung (Km), der vom Gehäuse gelesen wird, und daß die Prüfung der Echtheit des Datensatzes des Spieles eine Entschlüsselung im Inneren des Gehäuses mittels des Schlüssels für die Spielverschlüsselung umfaßt.

11. Verfahren nach den Ansprüchen 6 und 10, dadurch gekennzeichnet, daß man nur das Echtheitszertifikat (CTF) verschlüsselt und entschlüsselt.

12. Verfahren nach Anspruch 9 in Kombination mit dem Anspruch 10 oder 11, dadurch gekennzeichnet, daß man im Gehäuse den Schlüssel der Spielverschlüsselung (Km) speichert, nachdem er mittels des Schlüssels der Gehäuseverschlüsselung (Kf) verschlüsselt worden ist.

13. Verfahren nach Anspruch 9 in Kombination mit einem der Ansprüche 10 bis 13, dadurch gekennzeichnet, daß das Gerät mehrere Gehäuse und mehrere tragbare Gegenstände umfaßt, jedem Gehäuse ein anderer Schlüssel der Gehäuseverschlüsselung (Kf) zugeordnet ist, wohingegen der Schlüssel der Spielverschlüsselung (Km) allen Gehäusen und allen tragbaren Gegenständen gemeinsam ist, der Schlüssel der Gehäuseverschlüsselung eines Gehäuses in diesem vor der Speicherung des Schlüssels der Spielverschlüsselung gespeichert wird und der Datensatz des Spieles eines tragbaren Gegenstandes in diesem gespeichert wird, nachdem er wenigstens teilweise verschlüsselt worden oder einer Information (CTFc) zugeordnet worden ist, die wenigstens teilweise mittels des Schlüssels der Spielverschlüsselung verschlüsselt ist.

14. Verfahren nach Anspruch 9 oder einem der Ansprüche 10 bis 13, dadurch gekennzeichnet, daß der Schlüssel der Ergebnisverschlüsselung (Kr) der Schlüssel der Gehäuseverschlüsselung (Kf), oder der Schlüssel der Spielverschlüsselung (Km) ist, oder ausgehend von einer Kombination aus dem Schlüssel der Gehäuseverschlüsselung und dem Schlüssel der Spielverschlüsselung erhalten wird.

15. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß man im tragbaren Gegenstand, der mit dem Gehäuse zusammenarbeitet, eine Schlüsselinformation (ICR) speichert, die eineindeutig mit dem besagten Schlüssel der Ergebnisverschlüsselung in Zusammenhang steht, und daß die Gültigmachungsstation Zugang zu dem besagten Schlüssel der Ergebnisverschlüsselung hat, indem diese Schlüsselinformation, die im tragbaren Gegenstand gespeichert wird, eingelesen wird.

16. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der Datensatz des Spieles (JE) eines tragbaren Gegenstandes über ein Serienprotokoll zwischen dem tragbaren Gegenstand und dem Gehäuse gelesen wird.

17. Elektronisches Spielgerät, dadurch gekennzeichnet, daß es wenigstens ein Gehäuse (BT), wenigstens einen tragbaren Gegenstand (OB) und wenigstens eine Gültigmachungsstation (ST) umfaßt, daß der tragbare Gegenstand einen Spielspeicher (MJ), der einen Datensatz des Spieles (JE) enthält, dessen Echtheit bestätigt werden kann und der ein Spiel wiedergibt, einen Ergebnisspeicher (MR), der eine verschlüsselte Ergebnisinformation (IFRc) enthalten kann, eine erste Kommunikationsschnitt-

stelle (ESC), die mit einer Gehäusekommunikationsschnittstelle (ESB) zusammenarbeiten kann, und eine zweite Kommunikationsschnittstelle (ESC) umfaßt, die mit einer Stationskommunikationsschnittstelle (ESS) kommunizieren kann, das Gehäuse einen Schlüsselspeicher (MC), der einen Schlüssel für die Ergebnisverschlüsselung enthält, einen Arbeitsspeicher (MT), der zum Einschreiben und Auslesen zugänglich ist, und eine Verarbeitungseinheit (UT) umfaßt, die mit den Speichern sowie der Gehäusekommunikationsschnittstelle verbunden ist, wobei die Verarbeitungseinheit während der Zusammenarbeit zwischen der Gehäusekommunikationsschnittstelle und der ersten Kommunikationsschnittstelle des Gegenstandes die Echtheit des Datensatzes prüfen kann, der im Gegenstand gespeichert ist, und diesen Datensatz im Arbeitsspeicher speichern kann, um das Spiel auf der Höhe des Gehäuses ablaufen zu lassen, woraufhin eine Ergebnisinformation (IFR), die von dem Spiel abhängt, mit Hilfe des Schlüssels für die Ergebnisverschlüsselung verschlüsselt wird und diese verschlüsselte Ergebnisinformation (IFRc) an die Gehäusekommunikationsschnittstelle gelegt wird, um sie schließlich im Ergebnisspeicher des Gegenstandes zu speichern, und die Gültigmachungsstation (ST) Einrichtungen (PR), die den besagten Schlüssel der Ergebnisverschlüsselung bestimmen können und Stationsverarbeitungseinrichtungen (PR) umfaßt, die die verschlüsselte Ergebnisinformation über die Stationskommunikationsschnittstelle während der Zusammenarbeit zwischen dem tragbaren Gegenstand und der Station lesen können und eine Gültigkeitsverarbeitung ausgehend von wenigstens der verschlüsselten Ergebnisinformation und dem Schlüssel der Ergebnisverschlüsselung ausführen können.

18. Gerät nach Anspruch 17, dadurch gekennzeichnet, daß die Stationsverarbeitungseinrichtungen Stationsentschlüsselungseinrichtungen umfassen, die die verschlüsselte Ergebnisinformation entschlüsseln können.

19. Gerät nach Anspruch 17, dadurch gekennzeichnet, daß die Verarbeitungseinheit des Gehäuses gleichfalls die nicht verschlüsselte Ergebnisinformation an die Gehäusekommunikationsschnittstelle legen kann, um sie im Ergebnisspeicher des Gegenstandes zu speichern, und daß die Stationsverarbeitungseinrichtungen darüber hinaus so ausgebildet sind, daß sie die nicht verschlüsselte Ergebnisinformation über die Stationskommunikationsschnittstelle lesen und die Stationsverschlüsselungseinrichtungen, die die nicht verschlüsselte Ergebnisinformation mittels des Schlüssels der Ergebnisverschlüsselung verschlüsseln können, sowie die Vergleichseinrichtungen zum Vergleichen der neu berechneten verschlüsselten Ergebnisinformation mit der verschlüsselten Ergebnisinformation umfassen, die im Ergebnisspeicher des tragbaren Gegenstandes gespeichert ist.

20. Gerät nach einem der Ansprüche 17 bis 19, dadurch gekennzeichnet, daß die erste Kommunikationsschnittstelle (SEC) des tragbaren Gegenstandes eine serielle Schnittstelle ist.

21. Gerät nach einem der Ansprüche 17 bis 20, dadurch gekennzeichnet, daß der Datensatz des Spieles, dessen Echtheit bestätigt werden kann, einem Echtheitszertifikat zugeordnet wird, und daß die Einrichtungen zum Prüfen der Echtheit dieses Datensatzes des Spieles Einrichtungen zum Berechnen des Zertifikats, die das besagte Echtheitszertifikat ausgehend von dem Datensatz des Spieles neu berechnen können, und Vergleichseinrichtungen umfassen, die das neu berechnete Zertifikat und das Zertifikat vergleichen können, das im Spielspeicher des tragbaren Gegenstandes gespeichert ist.

22. Gerät nach einem der Ansprüche 17 bis 21, dadurch gekennzeichnet, daß es Verschlüsselungseinrichtungen umfaßt, die wenigstens teilweise den Datensatz des Spieles (JE), dessen Echtheit bestätigt werden kann, oder eine Information (CTF), die mit dem Datensatz des Spieles in Verbindung steht, ausgehend von wenigstens einem Schlüssel der Spielverschlüsselung verschlüsseln können, und daß der Schlüsselspeicher des Gehäuses diesen Schlüssel der Spielverschlüsselung enthalten kann, während die Einrichtungen zum Prüfen der Echtheit des Datensatzes des Spieles Entschlüsselungseinrichtungen umfassen, die mit dem Schlüsselspeicher verbunden sind.

23. Gerät nach den Ansprüchen 21 und 22, dadurch gekennzeichnet, daß die Verschlüsselungseinrichtungen nur das Echtheitszertifikat (CTF) verschlüsseln.

24. Gerät nach Anspruch 22 oder 23, dadurch gekennzeichnet, daß die Verschlüsselungseinrichtungen (CPU) im tragbaren Gegenstand aufgenommen sind.

25. Gerät nach einem der Ansprüche 22 bis 24, dadurch gekennzeichnet, daß der Schlüssel der Spielverschlüsselung verschlüsselt gespeichert ist und daß die Verarbeitungseinheit (UT) des Gehäuses Entschlüsselungseinrichtungen für diesen Schlüssel der Spielverschlüsselung umfaßt.

26. Gerät nach einem der Ansprüche 17 bis 25, dadurch gekennzeichnet, daß es Einrichtungen (CPU)

der Bestätigung der fehlenden Echtheit des Datensatzes des Spieles, dessen Echtheit bestätigt werden kann, des tragbaren Gegenstandes umfaßt.

27. Gerät nach einem der Ansprüche 17 bis 26, dadurch gekennzeichnet, daß es Einrichtungen (CPU) zum Verbieten des Einschreibens der verschlüsselten Ergebnisinformation in den Ergebnisspeicher des tragbaren Gegenstandes umfaßt.

28. Gerät nach Anspruch 26 oder 27, dadurch gekennzeichnet, daß die Einrichtungen (CPU) zur Bestätigung der fehlenden Echtheit und/oder die Verbotseinrichtungen (CPU) im tragbaren Gegenstand aufgenommen sind.

29. Gerät nach einem der Ansprüche 17 bis 28, dadurch gekennzeichnet, daß es mehrere Gehäuse, mehrere tragbare Gegenstände und mehrere Gültigmachungsstationen umfaßt, wobei irgendein tragbarer Gegenstand mit irgendeinem der Gehäuse und mit irgendeiner der Prüfstationen zusammenarbeiten kann.

Claims

1. Tamper protection and activation method for an electronic gaming device including at least one housing (BT), as well as at least one portable article (OB) capable of cooperating with the housing, in which method at least one result-encryption key is stored in the housing and an authenticatable set of digital game data (JE) representative of a game is stored in the portable article, the portable article is made to cooperate with the housing, the authentication of the set of game data is verified (8) within the housing and this set of game data is stored in a working memory (MT) of the housing, in such a way as to authorize the running (9) of the game in the housing, then, after the running of at least a part of the game, a result information item (IFR) dependent on the said game is encrypted (10) within the housing with the aid at least of the said result-encryption key, and this encrypted result information item (IFRc) is stored (11) in a result memory (MR) of the portable article, then, the portable article is made to cooperate with a validation station (ST) having access to the said result-encryption key, the said station performing a validation processing (13) on the basis at least of the said encrypted result information item and of the said result-encryption key.

2. Method according to Claim 1, characterized in that the validation process includes decryption of the encrypted result information items.

3. Method according to Claim 1, characterized in that the unencrypted result information item is stored in the portable article jointly with encrypted result information item, and in that the validation processing includes re-encryption of the unencrypted result information item stored in the portable article and a comparison of this re-encrypted result information item with the encrypted result information item stored in the result memory of the portable article.

4. Method according to one of Claims 1 to 3, characterized in that when the authentication of the set of game data of the portable article has been verified and the said set has been stored in the working memory of the housing, all subsequent utilization, by the housing, of the set of game data of this portable article is prohibited (20).

5. Method according to Claim 4, characterized in that, the device comprising several housings and several portable articles, when the authentication of the set of game data of one of the portable articles has been verified and when the said set has been stored in the working memory of one of the housings, all subsequent utilization, by any one of the housings, of the set of game data of this portable article is prohibited.

6. Method according to one of the preceding claims, characterized in that the set of game data stored in the portable article is authenticated by appending thereto an authentication certificate (CTF) linked in a one-to-one manner with the said set of game data (JE) and in that the verification of the authentication of the set of game data includes a recalculation of the authentication certificate within the housing and a comparison between the recalculated authentication certificate and the authentication certificate stored in the portable article.

7. Method according to Claim 4 or 5 taken in combination with Claim 6, characterized in that all subsequent utilization of a set of game data is prohibited by altering, in the corresponding portable article, at least partially the said authentication certificate and/or at least partially the set of game data.

8. Method according to one of the preceding claims taken in combination with Claim 4, characterized in that the storage of the encrypted result information item in the portable article is authorized (21) only if all subsequent utilization of the set of game data of this portable article has been previously prohibited.

9. Method according to one of the preceding claims, characterized in that a housing-encryption key (Kf) is stored in the housing.

10. Method according to one of the preceding claims,

characterized in that at least one game-encryption key (Km) is stored in the housing, in that the authentication of the set of game data stored in the portable article includes at least partial encryption of this set of game data, or of an information item (CTF) linked with this set of game data, with the aid of the game-encryption key (Km), before reading by the housing, and in that the verification of the authentication of this set of game data includes decryption within the housing with the aid of the game-encryption key.

11. Method according to Claims 6 and 10, characterized in that only the authentication certificate (CTF) is encrypted and decrypted.

12. Method according to Claim 9 taken in combination with Claim 10 or 11, characterized in that the game-encryption key (Km) having been encrypted with the aid of the housing-encryption key (Kf) is stored in the housing.

13. Method according to Claim 9 taken in combination with one of Claims 10 to 12, characterized in that, the device including several housings and several portable articles, a different housing-encryption key (Kf) is associated with each housing whilst the game-encryption key (Km) is common for all the housings and to all the portable articles, in that the housing-encryption key of a housing is stored in the latter before storage of the game-encryption key, and in that the set of game data of a portable article is stored in the latter, already at least partially encrypted, or associated with an information item (CTFc) already at least partially encrypted, with the aid of the game-encryption key.

14. Method according to Claim 9 or one of Claims 10 to 13, characterized in that the result-encryption key (Kr) is the housing-encryption key (Kf), or the game-encryption key (Km), or is obtained from a combination of the housing-encryption key and of the game-encryption key.

15. Method according to one of the preceding claims, characterized in that a key information item (ICR) associated in a one-to-one manner with the said result-encryption key is stored in the portable article cooperating with the housing, and in that the validation station has access to the said result-encryption key by reading the said key information item stored in the portable article.

16. Method according to one of the preceding claims, characterized in that the set of game data (JE) of a portable article is read by way of a serial protocol between the portable article and the housing.

17. Electronic gaming device, characterized in that it comprises at least one housing (BT), at least one portable article (OB), and at least one validation station (ST), in that the portable article includes a game memory (MJ) containing an authenticatable set of game data (JE) representing a game, a result memory (MR) able to contain an encrypted result information item (IFRc), a first communication interface (ESC) able to cooperate with a housing-communication interface (ESB), and a second communication interface (ESC) able to communicate with a station-communication interface (ESS), in that the housing includes a key memory (MC) containing a result-encryption key, a write- and read-accessible working memory (MT), and a processing unit (UT) linked to these memories as well as to the housing-communication interface, the processing unit being capable, during cooperation between the housing-communication interface and the first communication interface of the article, of verifying the authentication of the set of game data stored in the article and of storing the said set in the working memory so as to allow the running of the game in the housing, then of encrypting a result information item (IFR) dependent on the said game, with the aid of the result-encryption key, and of communicating this encrypted result information item (IFRc) to the housing-communication interface for the purposes of the storage thereof in the result memory of the article, and in that the validation station (ST) includes means (PR) able to determine the said result-encryption key and station-processing means (PR) able to read the encrypted result information item via the station-communication interface, during cooperation between the portable article and the station, and to perform a validation processing from at least this encrypted result information item and the result-encryption key.

18. Device according to Claim 17, characterized in that the station-processing means include station-decryption means able to decrypt the encrypted result information item.

19. Device according to Claim 17, characterized in that the processing unit of the housing is able also to communicate the unencrypted result information item to the housing-communication interface for the purposes of storage thereof in the result memory of the article, and in that the station-processing means are furthermore able to read the unencrypted result information item via the station-communication interface, and include station-encryption means able to encrypt the said unencrypted result information item with the aid of the result-encryption key, as well as comparison means for comparing the recalculated encrypted result information item with the encrypted result information item stored in the result memory of the portable article.

20. Device according to one of Claims 17 to 19, characterized in that the first communication interface (SEC) of the portable article is a serial interface.

21. Device according to one of Claims 17 to 20, characterized in that the authenticatable set of game data is associated with an authentication certificate and in that the means of verifying the authentication of this set of game data include certificate calculation means able to recalculate the said authentication certificate from the set of game data, and comparison means able to compare the recalculated certificate and the certificate stored in the game memory of the portable article.

22. Device according to one of Claims 17 to 21, characterized in that it comprises encryption means able to encrypt at least partially the set of authenticatable game data (JE), or an information item (CTF) linked with this set of game data, from at least one game-encryption key, and in that the key memory of the housing is able to contain the said game-encryption key whilst the means of verifying the authentication of the set of game data include decryption means linked to the key memory.

23. Device according to Claims 21 and 22, characterized in that the encryption means encrypt only the authentication certificate (CTF).

24. Device according to Claim 22 or 23, characterized in that the encryption means (CPU) are incorporated with the portable article.

25. Device according to one of Claims 22 to 24, characterized in that the game-encryption key is stored encrypted and in that the processing unit (UT) of the housing includes means for decrypting this game-encryption key.

26. Device according to one of Claims 17 to 25, characterized in that it comprises means (CPU) for invalidating the authenticatable set of game data of a portable article.

27. Device according to one of Claims 17 to 26, characterized in that it comprises means (CPU) for prohibiting the writing of the encrypted result information item to the result memory of the portable article.

28. Device according to Claim 26 or 27, characterized in that the invalidation means (CPU) and/or the prohibiting means (CPU) are incorporated into the portable article.

29. Device according to one of Claims 17 to 28, characterized in that it comprises several housings, several portable articles and several validation stations, any one of the portable articles being capable of cooperating with any one of the housings and with any one of the validation stations.

FIG_1

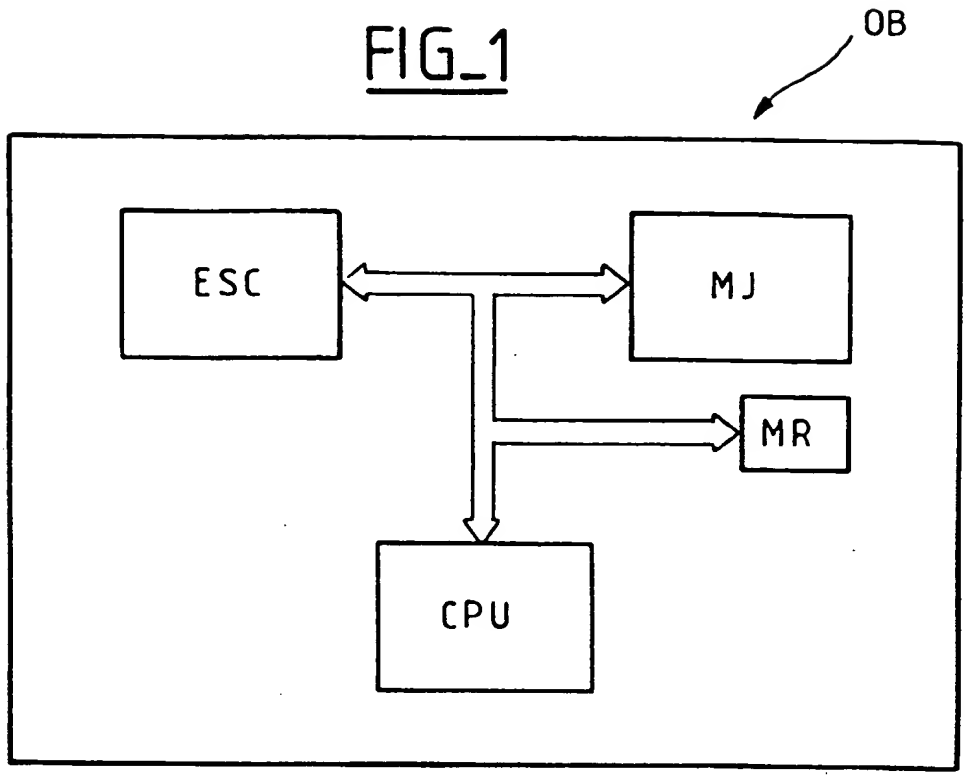


FIG_2

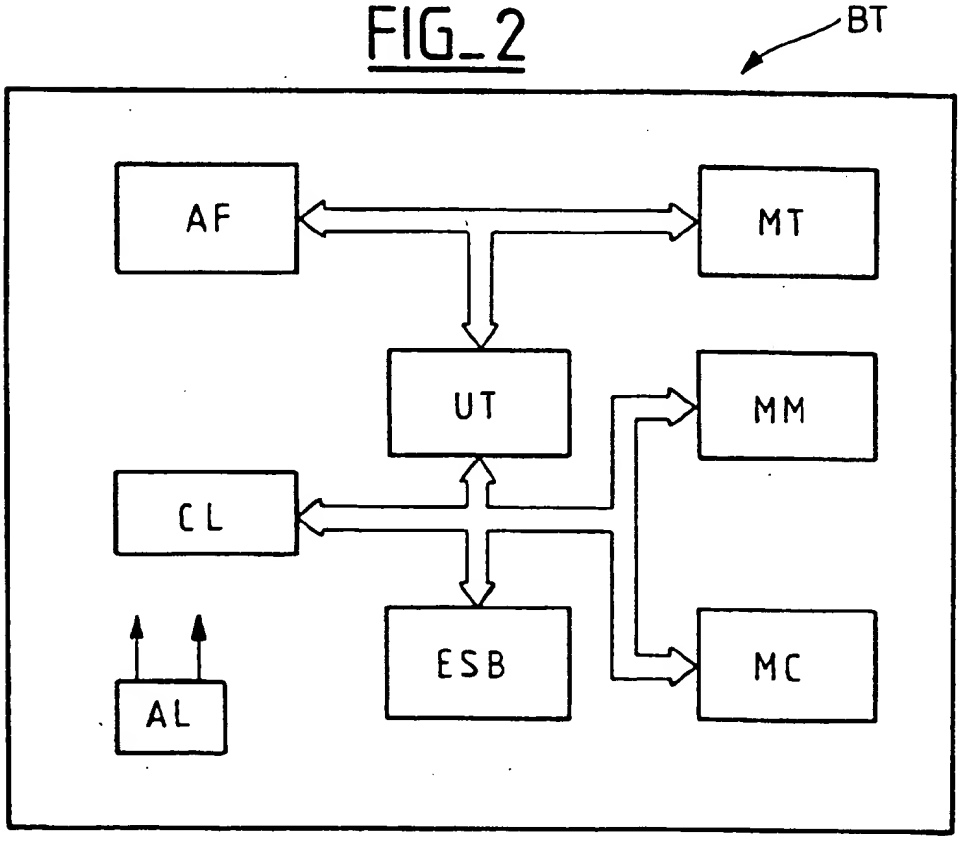


FIG_3

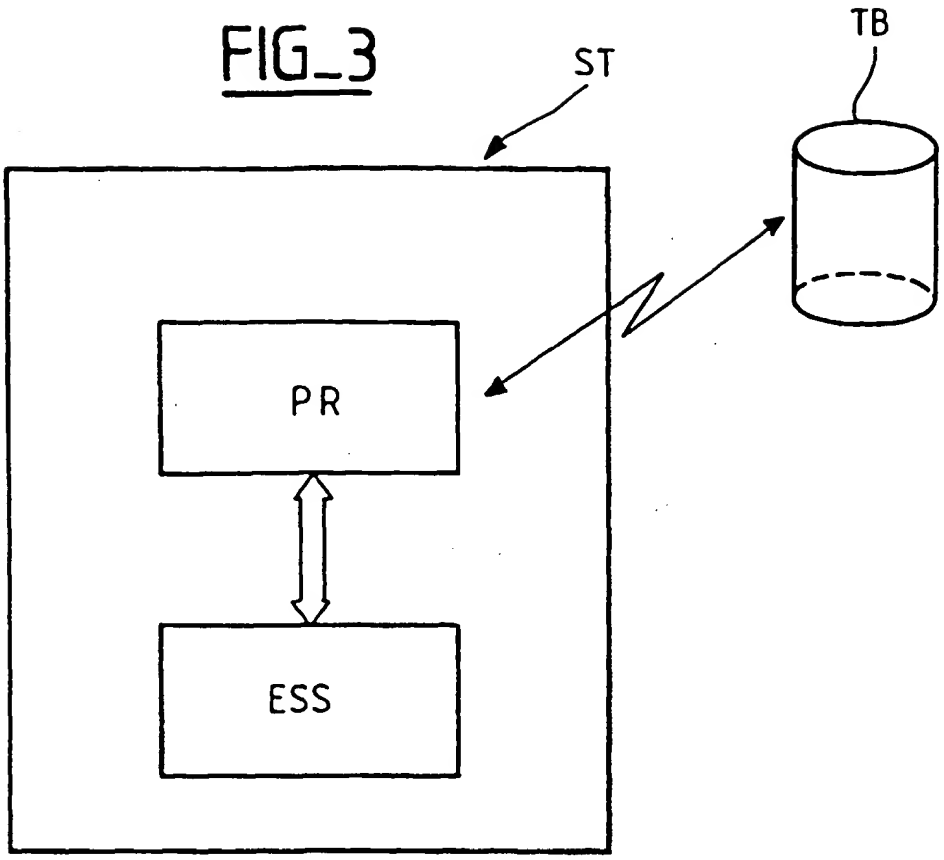


FIG_4a

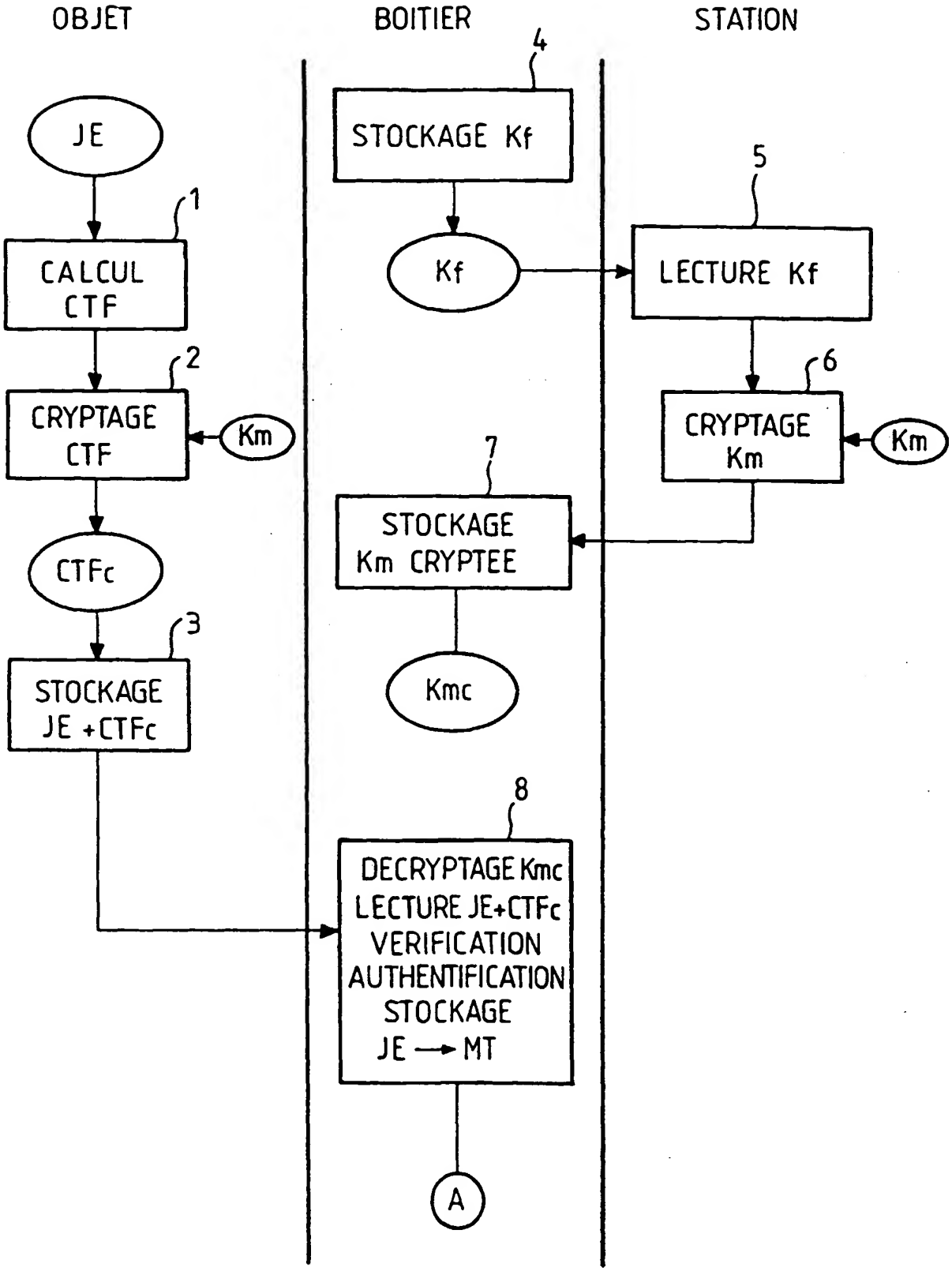

OBJET
BOITIER
STATION
JE
1
CALCUL CTF
2
CRYPTAGE CTF
Km
CTFc
3
STOCKAGE JE +CTFc
4
STOCKAGE Kf
Kf
5
LECTURE Kf
6
CRYPTAGE Km
Km
7
STOCKAGE Km CRYPTEE
Kmc
8
DECRYPTAGE Kmc
LECTURE JE+CTFc
VERIFICATION
AUTHENTIFICATION
STOCKAGE
JE → MT
A

FIG_4b

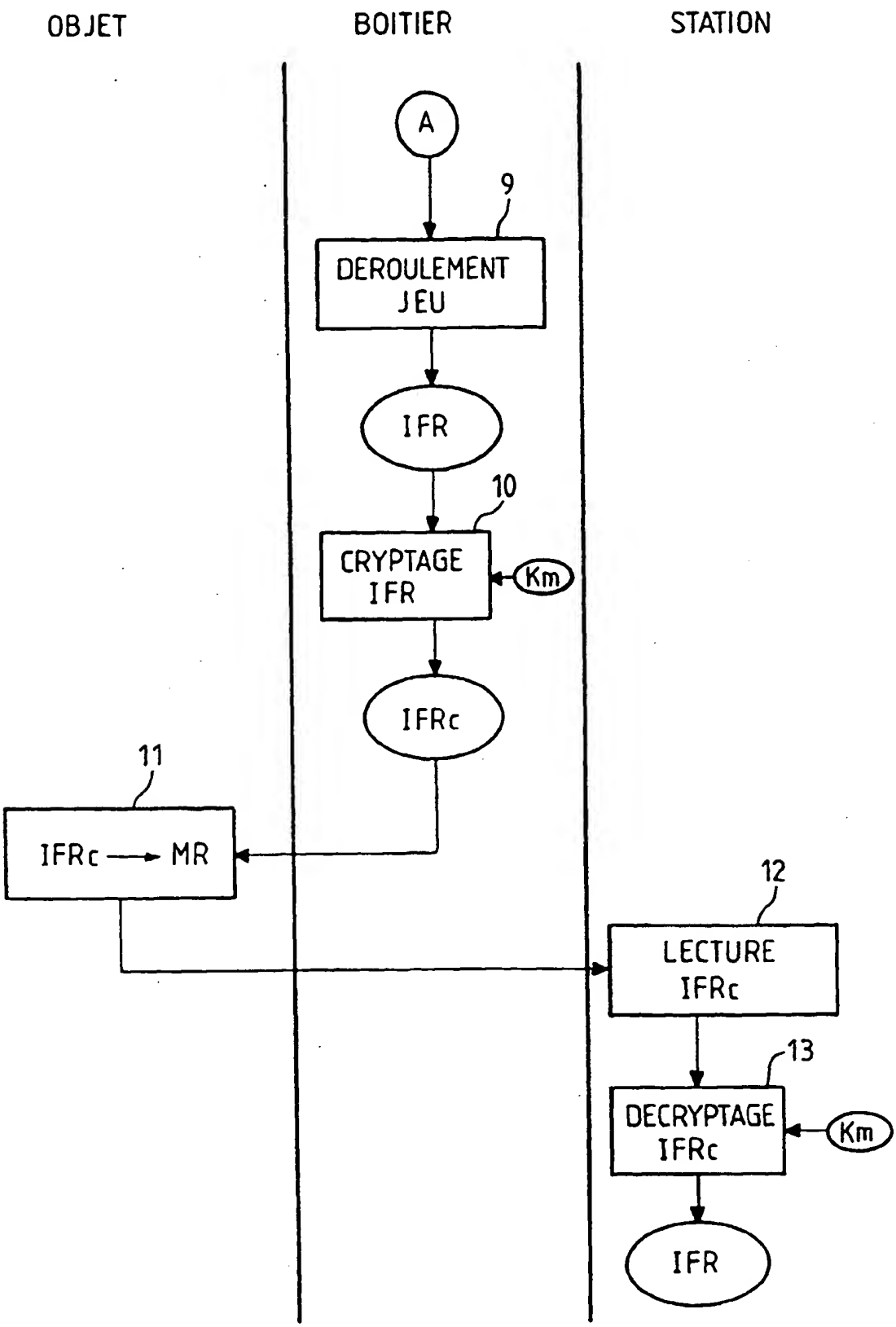

OBJET
BOITIER
STATION
A
9
DEROULEMENT JEU
IFR
10
CRYPTAGE IFR
Km
IFRc
11
IFRc → MR
12
LECTURE IFRc
13
DECRYPTAGE IFRc
Km
IFR

FIG_5

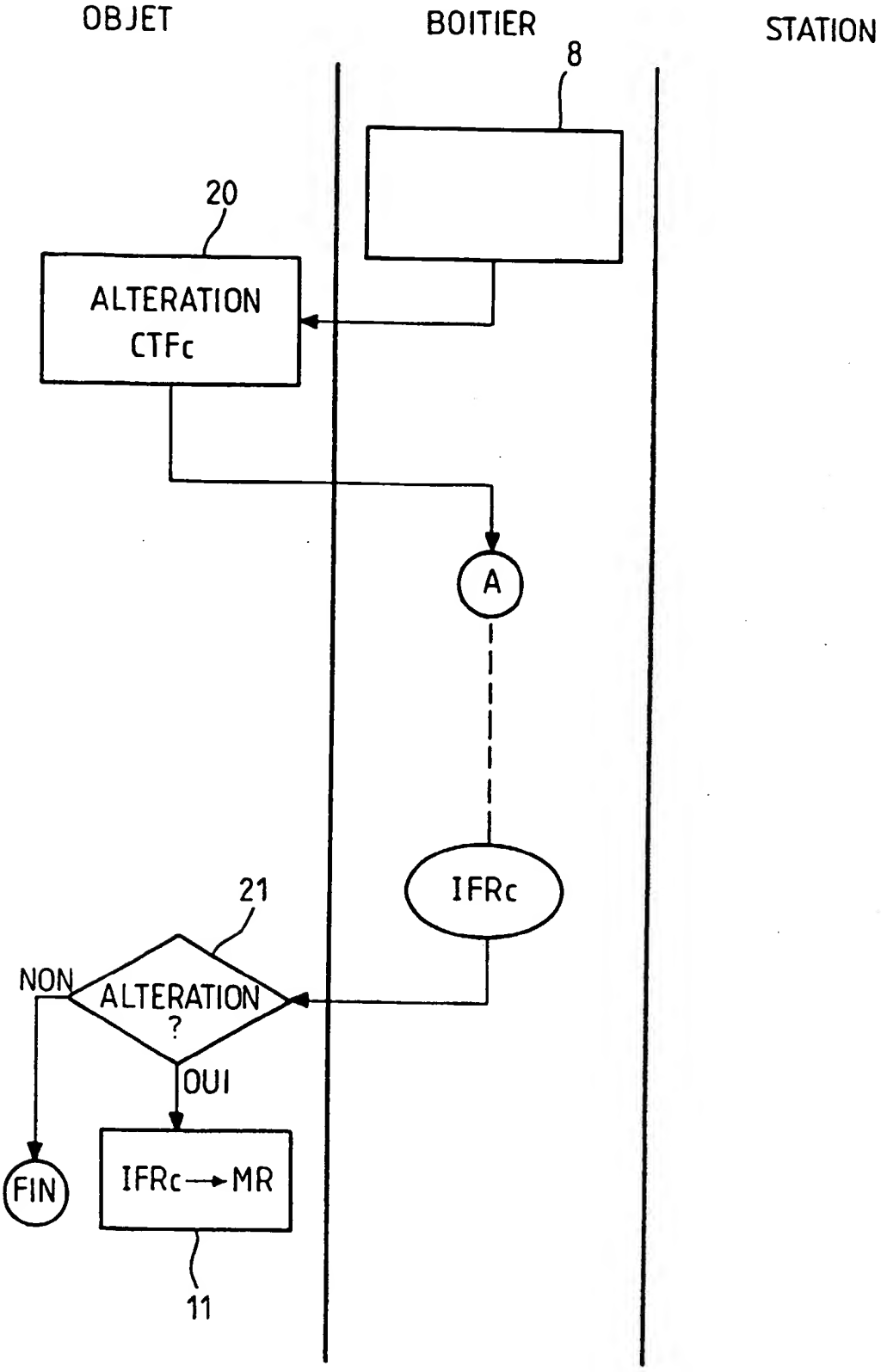
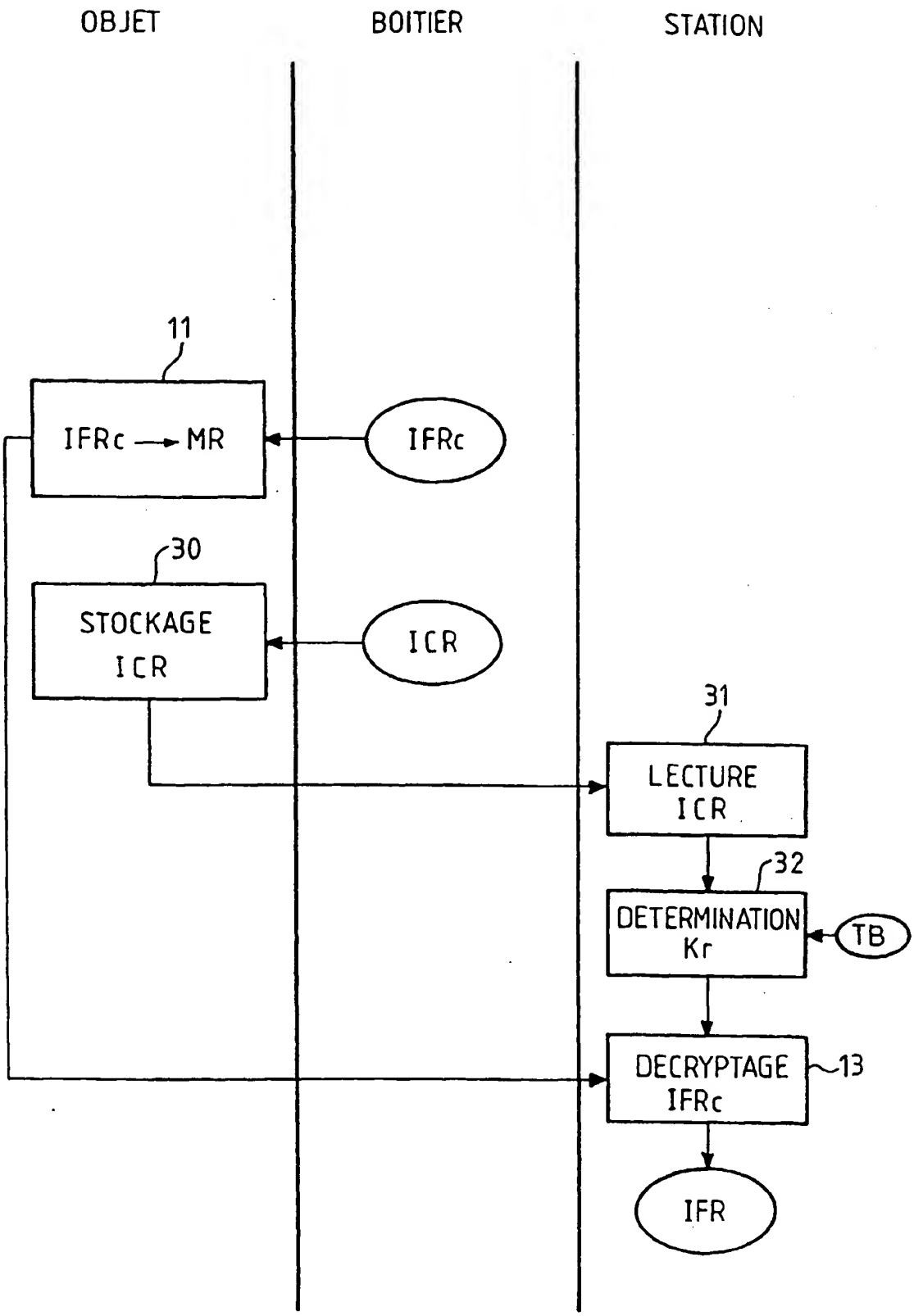

OBJET
BOITIER
STATION
8
20
ALTERATION
CTFc
A
IFRc
21
NON
ALTERATION
?
OUI
FIN
IFRc → MR
11

FIG_6


OBJET
BOITIER
STATION
11
IFRc → MR
IFRc
30
STOCKAGE ICR
ICR
31
LECTURE ICR
32
DETERMINATION Kr
TB
DECRYPTAGE IFRc
13
IFR